WHAT IS CLAIMED IS:

1. A quantitative competition method in which the minimum one V_{MIN} of all users' intended values V_{vi} selected from among M monotone increasing values V_w, where w=1,2,..., M, in the range of predetermined lower-limit and upper-limit values V_1 and V_M and only a user j having selected said minimum value W_{MIN} as his intended value are specified by a plurality of user apparatuses i, where i=1,..., N, said N being an integer equal to or larger than 2, first and second quantitative competition apparatuses, and a bulletin board apparatus that makes public information received from said plurality of user apparatuses and said first and second quantitative competition apparatuses, said method comprising:

Step (a) wherein each of said user apparatuses i: responds to said intended value V_{vi} input from one of said all users to generate two M-element sequences of information s_i and t_i whose corresponding elements equal at values in the range from said lower-limit value V_1 or larger to said intended value V_{vi} or smaller and differ at values in the range from said intended value V_{vi} or larger to said upper-limit value V_M or smaller; and secretly sends information about said two M-element sequences of information s_i and t_i to said first and second quantitative competition apparatuses, respectively, said M representing the number of values selectable as said intended values in the range from said lower-limit value V_1 or larger to said upper-limit value V_M or smaller;

Step (b) wherein said first quantitative competition apparatus: extracts, for a given value V_w equal to or larger than said lower-limit value V_1 and equal to or smaller than said upper-limit value, those elements $s_{i,w}$ of said M-element sequences of information s_i sent from said all user apparatuses which correspond to w; and generates an element concatenation $Seq_{s,w}=s_{1,w}||s_{2,w}||\ldots||s_{N,w}$ in which said extracted elements $s_{i,w}$ are arranged in a predetermined order, said || representing the concatenation of data;

Step (c) wherein said second quantitative competition apparatus: extracts, for said given value V_w, those elements $t_{i,w}$ of said M-element sequences of information t_i sent from said all user apparatuses which correspond to said value w; and generates an element concatenation $Seq_{t,w}=t_{1,w}||t_{2,w}||\ldots||t_{N,w}$ in which said extracted elements $t_{i,w}$ are arranged in a predetermined order;

Step (d) wherein said bulletin board apparatus: compares said element concatenations $Seq_{s,w}$ and $Seq_{t,w}$ without revealing their values; decides the presence or absence of a user having selected his intended value equal to or smaller than said value V_w, depending on whether said concatenations $Seq_{s,w}$ and $Seq_{t,w}$ differ or equal; determines the minimum intended value V_{MIN} by changing said value w based on said decision and makes the value MIN public; and

Step (e) wherein said first and second quantitative competition apparatuses send element concatenations $Seq_{s,MIN}$ and $Seq_{t,MIN}$, respectively, to said bulletin board apparatus to make them public, whereby allowing each user to identify user j who committed the minimum intended value V_{MIN} by finding j which satisfies $s_{j,MIN}\neq t_{j,MIN}$ of the corresponding elements in said element concatenations $Seq_{s,MIN}$ and $Seq_{t,MIN}$.

2. The method of claim 1, wherein:

said Step (a) includes: a step wherein said user apparatus of said each user i generates random numbers $R1_i$ and $R2_i$ secretly send a pair of information $(R1_i, s_i)$ to said first quantitative competition apparatus and a pair of information $(R2_i, t_i)$ to said second quantitative competition apparatus; and a step wherein said user apparatus calculates hash values $H1_i=h(R1_i||s_i)$ and $H2_i=h(R2_i||t_i)$ of concatenations $R1_i||s_i$ and $R2_i||t_i$ of said pairs of information $(R1_i, s_i)$ and $(R2_i, t_i)$ by a hash function h, and sends said hash values $H1_i$ and

$H2_i$ to said bulletin board apparatus; and

said Step (d) includes a step wherein said bulletin board apparatus makes public said hash values $H1_i$ and $H2_i$, where i=1,2, …, N, as commitments of said all users.

3. The method of claim 2, wherein:

said Step (b) includes a step wherein said first quantitative competition apparatus: calculates a hash value $HS_w=h(Seq_{s,w})$ of said element concatenation $Seq_{s,w}$ by said hash function h; and sends said hash value HS_w to said bulletin board apparatus;

said Step (c) includes a step wherein said second quantitative competition apparatus: calculates a hash value $HT_w=h(Seq_{t,w})$ of said element concatenation $Seq_{t,w}$ by said hash function h; and sends said hash value HT_w to said bulletin board apparatus; and

said Step (d) includes a step wherein said bulletin board apparatus: makes public and compares said hash values HS_w and HT_w received from said first and second quantitative competition apparatuses; decides the presence or absence of a user having selected his intended value equal to or smaller than said value V_w, depending on whether said hash values HS_w and HT_w differ or equal; and determines said minimum intended value V_{MIN} by changing said value w based on said decision.

4. The method of claim 2, wherein:

said first and second quantitative competition apparatuses have stored therein a prime P made public previously by said bulletin board apparatus, said prime P being a prime such that P−1 has a large prime as its divisor, and said first and second quantitative competition apparatuses having selected a common integral value w;

said Step (b) includes a step wherein said first quantitative competition apparatus: calculates a hash value $HS_w=h'(Seq_{s,w})$ of said element concatenation $Seq_{s,w}$ by a hash function h' that maps an arbitrary integer over a finite field uniquely and randomly; generates a random number RA_w; calculates a hash value $HA_w=h(RA_w||HS_w)$ of a concatenation $RA_w||HS_w$ by said hash function h; calculates HS_w^{RAw}(mod P); and sends a pair (HA_w, HS_w^{RAw}(mod P)) of said hash value HA_w and said value HS_w^{RAw}(mod P) to said bulletin board apparatus;

said Step (c) includes a step wherein said second quantitative competition apparatus: calculates a hash value $HT_w=h'(Seq_{t,w})$ of said element concatenation $Seq_{t,w}$ by a hash function h'; generates a random number RB_w; calculates a hash value $HB_w=h(RB_w||HT_w)$ of a concatenation $RB_w||HT_w$ by said hash function h; calculates HT_w^{RBw}(mod P); and sends a pair (HB_w, HT_w^{RBw}(mod P)) of said hash value HB_w and said value HT_w^{RBw}(mod P) to said bulletin board apparatus; and

said Step (d) includes: a step wherein said first quantitative competition apparatus reads said HT_w^{RBw}(mod P) from said bulletin board apparatus, and calculates and sends $(HT_w^{RBw})^{RAw}$(mod P) to said bulletin board apparatus; a step wherein said second quantitative competition apparatus reads said HS_w^{RAw}(mod P) from said bulletin board apparatus, and calculates and sends $(HS_w^{RAw})^{RBw}$(mod P) to said bulletin board apparatus; and a step wherein said bulletin board apparatus: makes public and compares said $(HS_w^{RAw})^{RBw}$(mod P) and $(HT_w^{RBw})^{RAw}$(mod P) received from said first and second quantitative competition apparatuses; decides the presence or absence of a user having selected his intended value equal to or smaller than said value V_w, depending on whether said $(HS_w^{RAw})^{RBw}$(mod P) and $(HT_w^{RBw})^{RAw}$(mod P) differ or equal; and determines said minimum intended value V_{MIN} by changing said value w based on said decision.

5. The method of claim 3 or 4, wherein: letting w_{min} and w_{max} represent variables, said first and second quantitative competition apparatuses

have said value w in common as the maximum integer equal to or smaller than $(w_{min}+w_{max})/2=(1+M)/2$ where $w_{min}=1$ and $w_{max}=M$; and

said Step (d) includes a step wherein: w is substituted for said variable w_{max} or w+1 is substituted for said variable w_{min}, depending on the presence or absence of a user having selected his intended value equal to or smaller than said value V_w; said Steps (b) and (c) are repeated until $w_{max}=w_{min}=MIN$ to obtain said minimum intended value V_{MIN} corresponding to said value MIN; and upon each repetition of said Steps (b) and (c), said bulletin board apparatus makes public the results of calculation.

6. The method of claim 4, wherein each element of said M-element sequences of information s_i and t_i is a one-bit element.

7. The method of claim 4 or 6, said step (e) further comprising a step wherein said first and second quantitative competition apparatus send said bulletin board apparatus random numbers RA_{MIN} and RB_{MIN} and make them public.

8. The method of any one of claims 1 to 4, wherein: L quantitative competition apparatuses are provided, said L being equal to or larger than 3;

said Step (a) includes a step wherein when supplied with said value V_{vi}, said each user apparatus generates L sequences of information s_{ik}, where k=1,2, …, L, said L sequences of information s_{ik} being such that they are equal in all pieces of information corresponding to values equal to or greater than V_1 and equal to or smaller than V_{vi} but different in all pieces of information corresponding to values equal to or larger than V_{vi} and equal to or smaller than V_M and such that said value V_{vi} can be detected when at least two sequences s_{ia} and s_{ib} of said L sequences of information s_{ik} are known, where a≠b; and said each user apparatus sends said L sequences of information s_{ik} to a k-th quantitative competition apparatus; and

wherein two of said L quantitative competition apparatuses conduct quantitative competition, and when one of said two quantitative competition apparatuses goes down, another normal one of the remaining quantitative competition apparatuses is used to continue said quantitative competition.

9. The method of claim 1, wherein said Step (a) includes a step wherein: said each user apparatus secretly sends seed values s'_i and t'_i as information corresponding to said two sequences of information s_i and t_i to said first and second quantitative competition apparatuses, respectively; letting vi represent the element number corresponding to said intended value V_{vi}, said seed values s'_i and t'_i are determined by a one-way function F so that $F^d(s'_i)= F^d(t'_i)$, where $d=0,1, \ldots, M-vi$, and $F^e(s'_i)= F^e(t'_i)$, where $e= M-vi+1, \ldots, M-1$; and said two sequences of information s_i and t_i are given by the following equations

$s_i=\{s_{i,1}=F^{M-1}(s'_i), s_{i,2}=F^{M-2}(s'_i), \ldots, s_{i,vi-1}=F^{M-vi+1}(s'_i), s_{i,vi}=F^{M-vi}(s'_i), \ldots,$

$s_{i,M-1}=F(s'_i), s_{i,M}=s'_i\}$ and

$t_i=\{t_{i,1}=F^{M-1}(t'_i), t_{i,2}=F^{M-2}(t'_i), \ldots, t_{i,vi-1}=F^{M-vi+1}(t'_i), t_{i,vi}=F^{M-vi}(t'_i), \ldots,$

$t_{i,M-1}=F(t'_i), t_{i,M}=s'_i\}$.

10. The method of claim 1, wherein said Step (a) includes:

a step wherein said each user apparatus generates initial random numbers $R1_i$, $R2_i$, ca_i, cb_i, $s_{i,M+1}$ and $t_{i,M+1}$; and

a step wherein said each user apparatus: sets an initial value of m at M, and performs, with respect to the element number vi corresponding to said intended value V_{vi}, the following calculations

$$s_{i,m}=h(s_{i,m+1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i)) \text{ and}$$

$$t_{i,m}=h(t_{i,m+1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i))$$

sequentially for $m=M, M-1, \ldots, vi$ to provide subsequences $s_{i,m}\neq t_{i,m}$; calculates a sequence element for $m=vi-1$

$$s_{i,m}=t_{i,m}=h(s_{i,m-1}||t_{i,m-1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i))$$

and a sequence element for $m=vi-2, vi-3, \ldots, 0$

$s_{i,m}=t_{i,m}=h(s_{i,m-1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i))$

to provide subsequences $s_{i,m}=t_{i,m}$; and obtains sequences of said elements $s_{i,m}$ and $t_{i,m}$ as said sequences of information s_i and t_i, and a value $s_{i,0}$ for m=0; and

wherein said Step (a) further includes: a step wherein said each user apparatus encrypts $R1_i$ and $s_i=\{s_{i,1}, s_{i,2}, \ldots, s_{i,M}\}$ by an encryption function E_A, sends the resulting $E_A(s_i||R1_i)$ to said first quantitative competition apparatus, encrypts $R2_i$ and $t_i=\{t_{i,1}, t_{i,2}, \ldots, t_{i,M}\}$ by an encryption function E_B, and sends the resulting $E_B(t_i||R2_i)$ to said second quantitative competition apparatus; and a step wherein said each user apparatus sends $H1_i=h(s_i||R1_i)$, $H2_i=h(t_i||R2_i)$, $s_{i,0}$, $h^{M+1}(ca_i)$ and $h^{M+1}(cb_i)$ to said bulletin board to make them public.

11. A quantitative competition method in which the maximum one V_{MAX} of all users' intended values V_{vi} selected from among M monotone increasing values V_w, where w=1,2,..., M, in the range of predetermined lower-limit and upper-limit values V_1 and V_M and only a user j having selected said maximum value W_{MAX} as his intended value are specified by a plurality of user apparatuses i, where i=1,..., N, said N being an integer equal to or larger than 2, first and second quantitative competition apparatuses, and a bulletin board apparatus that makes public information received from said plurality of user apparatuses and said first and second quantitative competition apparatuses, said method comprising:

Step (a) wherein each of said user apparatuses i: responds to said intended value V_{vi} input from one of said all users to generate two M-element sequences of information s_i and t_i whose corresponding elements equal at values in the range from said lower-limit value V_1 or larger to said intended value V_{vi} or smaller and differ at values in the range from said intended value V_{vi} or larger to said upper-limit value V_M or smaller; and secretly sends information about said two M-element sequences of information s_i and t_i to said first and second quantitative competition apparatuses, respectively, said

M representing the number of values selectable as said intended values in the range from said lower-limit value V_1 or larger to said upper-limit value V_M or smaller;

Step (b) wherein said first quantitative competition apparatus: extracts, for a given value V_w equal to or larger than said lower-limit value V_1 and equal to or smaller than said upper-limit value, those elements $s_{i,w}$ of said M-element sequences of information s_i sent from said all user apparatuses which correspond to w; and generates an element concatenation $Seq_{s,w}=s_{1,w}||s_{2,w}||\ldots||s_{N,w}$ in which said extracted elements $s_{i,w}$ are arranged in a predetermined order, said || representing the concatenation of data;

Step (c) wherein said second quantitative competition apparatus: extracts, for said given value V_w, those elements $t_{i,w}$ of said M-element sequences of information t_i sent from said all user apparatuses which correspond to said value w; and generates an element concatenation $Seq_{t,w}=t_{1,w}||t_{2,w}||\ldots||t_{N,w}$ in which said extracted elements $t_{i,w}$ are arranged in a predetermined order;

Step (d) wherein said bulletin board apparatus: compares said element concatenations $Seq_{s,w}$ and $Seq_{t,w}$ without revealing their values; decides the presence or absence of a user having selected his intended value equal to or larger than said value V_w, depending on whether said concatenations $Seq_{s,w}$ and $Seq_{t,w}$ differ or equal; determines the maximum intended value V_{MAX} by changing said value w based on said decision and makes the value MAX public; and

Step (e) wherein said first and second quantitative competition apparatuses send element concatenations $Seq_{s,MAX}$ and $Seq_{t,MAX}$, respectively, to said bulletin board apparatus to make them public, whereby allowing each user to identify user j who committed the maximum intended value V_{MAX} by finding j which satisfies $s_{j,MAX}\neq t_{j,MAX}$ of the corresponding elements in said element concatenations $Seq_{s,MAX}$ and $Seq_{t,MAX}$.

12. The method of claim 11, wherein:

said Step (a) includes: a step wherein said user apparatus of said each user i generates random numbers $R1_i$ and $R2_i$ secretly send a pair of information $(R1_i, s_i)$ to said first quantitative competition apparatus and a pair of information $(R2_i, t_i)$ to said second quantitative competition apparatus; and a step wherein said user apparatus calculates hash values $H1_i=h(R1_i||s_i)$ and $H2_i=h(R2_i||t_i)$ of concatenations $R1_i||s_i$ and $R2_i||t_i$ of said pairs of information $(R1_i, s_i)$ and $(R2_i, t_i)$ by a hash function h, and sends said hash values $H1_i$ and $H2_i$ to said bulletin board apparatus; and

said Step (d) includes a step wherein said bulletin board apparatus makes public said hash values $H1_i$ and $H2_i$, where $i=1,2, \ldots, N$, as commitments of said all users.

13. The method of claim 12, wherein:

said Step (b) includes a step wherein said first quantitative competition apparatus: calculates a hash value $HS_w=h(Seq_{s,w})$ of said element concatenation $Seq_{s,w}$ by said hash function h; and sends said hash value HS_w to said bulletin board apparatus;

said Step (c) includes a step wherein said second quantitative competition apparatus: calculates a hash value $HT_w=h(Seq_{t,w})$ of said element concatenation $Seq_{t,w}$ by said hash function h; and sends said hash value HT_w to said bulletin board apparatus; and

said Step (d) includes a step wherein said bulletin board apparatus: makes public and compares said hash values HS_w and HT_w received from said first and second quantitative competition apparatuses; decides the presence or absence of a user having selected his intended value equal to or larger than said value V_w, depending on whether said hash values HS_w and HT_w differ or equal; and determines said maximum intended value V_{MAX} by changing said value w based on said decision.

14. The method of claim 12, wherein:

said first and second quantitative competition apparatuses have stored therein a prime P made public previously by said bulletin board apparatus, said prime P being a prime such that P−1 has a large prime as its divisor, and said first and second quantitative competition apparatuses having selected a common integral value w;

said Step (b) includes a step wherein said first quantitative competition apparatus: calculates a hash value $HS_w=h'(Seq_{s,w})$ of said element concatenation $Seq_{s,w}$ by a hash function h' that maps an arbitrary integer over a finite field uniquely and randomly; generates a random number RA_w; calculates a hash value $HA_w=h(RA_w||HS_w)$ of a concatenation $RA_w||HS_w$ by said hash function h; calculates HS_w^{RAw}(mod P); and sends a pair (HA_w, HS_w^{RAw}(mod P)) of said hash value HA_w and said value HS_w^{RAw}(mod P) to said bulletin board apparatus;

said Step (c) includes a step wherein said second quantitative competition apparatus: calculates a hash value $HT_w=h'(Seq_{t,w})$ of said element concatenation $Seq_{t,w}$ by a hash function h'; generates a random number RB_w; calculates a hash value $HB_w=h(RB_w||HT_w)$ of a concatenation $RB_w||HT_w$ by said hash function h; calculates HT_w^{RBw}(mod P); and sends a pair (HB_w, HT_w^{RBw}(mod P)) of said hash value HB_w and said value HT_w^{RBw}(mod P) to said bulletin board apparatus; and

said Step (d) includes: a step wherein said first quantitative competition apparatus reads said HT_w^{RBw}(mod P) from said bulletin board apparatus, and calculates and sends $(HT_w^{RBw})^{RAw}$(mod P) to said bulletin board apparatus; a step wherein said second quantitative competition apparatus reads said HS_w^{RAw}(mod P) from said bulletin board apparatus, and calculates and sends $(HS_w^{RAw})^{RBw}$(mod P) to said bulletin board apparatus;

and a step wherein said bulletin board apparatus: makes public and compares said $(HS_w^{RAw})^{RBw}$(mod P) and $(HT_w^{RBw})^{RAw}$(mod P) received from said first and second quantitative competition apparatuses; decides the presence or absence of a user having selected his intended value equal to or larger than said value V_w, depending on whether said $(HS_w^{RAw})^{RBw}$(mod P) and $(HT_w^{RBw})^{RAw}$(mod P) differ or equal; and determines said maximum intended value V_{MAX} by changing said value w based on said decision.

15. The method of claim 13 or 14, wherein: letting w_{min} and w_{max} represent variables of integers 1 to M, said first and second quantitative competition apparatuses have said value w in common as the maximum integer equal to or smaller than $(w_{min}+w_{max})/2=(1+M)/2$ where $w_{min}=1$ and $w_{max}=M$; and

said Step (d) includes a step wherein: w is substituted for said variable w_{max} or w+1 is substituted for said variable w_{min}, depending on the presence or absence of a user having selected his intended value equal to or larger than said value V_w; said Steps (b) and (c) are repeated until $w_{max}=w_{min}=MAX$ to obtain said minimum intended value V_{MAX} corresponding to said value MAX; and upon each repetition of said Steps (b) and (c), said bulletin board apparatus makes public the results of calculation.

16. The method of claim 14, wherein each element of said M-element sequences of information s_i and t_i is a one-bit element.

17. The method of claim 14 or 16, said step (e) further comprising a step wherein said first and second quantitative competition apparatus send said bulletin board apparatus random numbers RA_{MIN} and RB_{MIN}, respectively, to make them public.

18. The method of any one of claims 11 to 14, wherein: L quantitative competition apparatuses are provided, said L being equal to or larger than 3;

said Step (a) includes a step wherein when supplied with said value

V_{vi}, said each user apparatus generates L sequences of information s_{ik}, where k=1,2, …, L, said L sequences of information s_{ik} being such that they are equal in all pieces of information corresponding to values equal to or greater than V_1 and smaller than V_{vi} but different in all pieces of information corresponding to values equal to or larger than V_{vi} and equal to or smaller than V_M and such that said value V_{vi} can be detected when at least two sequences s_{ia} and s_{ib} of said L sequences of information s_{ik} are known, where a≠b; and said each user apparatus sends said L sequences of information s_{ik} to a k-th quantitative competition apparatus; and

wherein two of said L quantitative competition apparatuses conduct quantitative competition, and when one of said two quantitative competition apparatuses goes down, another normal one of the remaining quantitative competition apparatuses is used to continue said quantitative competition.

19. The method of claim 11, wherein said Step (a) includes a step wherein: said each user apparatus secretly sends seed values s'_i and t'_i as information corresponding to said two sequences of information s_i and t_i to said first and second quantitative competition apparatuses, respectively; letting vi represent the element number corresponding to said intended value V_{vi}, said seed values s'_i and t'_i are determined by a one-way function F so that $F^d(s'_i)= F^d(t'_i)$, where d=0,1, …, M−vi, and $F^e(s'_i)= F^e(t'_i)$, where e= M−vi+1, …, M−1; and said two sequences of information s_i and t_i are given by the following equations

$s_i=\{s_{i,1}=F^{M-1}(s'_i), s_{i,2}=F^{M-2}(s'_i), \ldots, s_{i,vi-1}=F^{M-vi+1}(s'_i), s_{i,vi}=F^{M-vi}(s'_i), \ldots,$
$s_{i,M-1}=F(s'_i), s_{i,M}=s'_i\}$ and

$t_i=\{t_{i,1}=F^{M-1}(t'_i), t_{i,2}=F^{M-2}(t'_i), \ldots, t_{i,vi-1}=F^{M-vi+1}(t'_i), t_{i,vi}=F^{M-vi}(t'_i), \ldots,$
$t_{i,M-1}=F(t'_i), t_{i,M}=s'_i\}$.

20. The method of claim 11, wherein said Step (a) includes:

a step wherein said each user apparatus generates initial random numbers $R1_i$, $R2_i$, ca_i, cb_i, $s_{i,M+1}$ and $t_{i,M+1}$; and

a step wherein said each user apparatus: sets an initial value of m at M, and performs, with respect to the element number vi corresponding to said intended value V_{vi}, the following calculations

$$s_{i,m}=h(s_{i,m+1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i)) \text{ and}$$
$$t_{i,m}=h(t_{i,m+1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i))$$

sequentially for m=M, M−1, ..., vi to provide subsequences $s_{i,m}\neq t_{i,m}$; calculates a sequence element for m=vi-1

$$s_{i,m}=t_{i,m}=h(s_{i,m-1}||t_{i,m-1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i))$$

and a sequence element for m=vi−2, vi−3, ..., 0

$$s_{i,m}=t_{i,m}=h(s_{i,m-1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i))$$

to provide subsequences $s_{i,m}=t_{i,m}$; and obtains sequences of said elements $s_{i,m}$ and $t_{i,m}$ as said sequences of information s_i and t_i, and a value $s_{i,0}$ for m=0; and

wherein said Step (a) further includes: a step wherein said each user apparatus encrypts $R1_i$ and $s_i=\{s_{i,1}, s_{i,2}, ..., s_{i,M}\}$ by an encryption function E_A, sends the resulting $E_A(s_i||R1_i)$ to said first quantitative competition apparatus, encrypts $R2_i$ and $t_i=\{t_{i,1}, t_{i,2}, ..., t_{i,M}\}$ by an encryption function E_B, and sends the resulting $E_B(t_i||R2_i)$ to said second quantitative competition apparatus; and a step wherein said each user apparatus sends $H1_i=h(s_i||R1_i)$, $H2_i=h(t_i||R2_i)$, $s_{i,0}$, $h^{M+1}(ca_i)$ and $h^{M+1}(cb_i)$ to said bulletin board to make them public.

21. The method of claim 1 or 11, wherein said Step (a) includes a step wherein said each user apparatus: generates a random number r_i; determines two pieces of random information a_i and b_i, where $r_i=a_i*b_i$, said symbol * being a predetermined common operator; sends said pieces of random information a_i and b_i to said first and second quantitative competition apparatuses, respectively; hashes said pieces of random information a_i and b_i by a hash function h; and sends hash values $h(a_i)$, $h(b_i)$ and $h(V_{vi}||r_i)$ to said bulletin board apparatus; and said Step (e) includes a step wherein said first

and second quantitative apparatuses send said pieces of random information a_j and b_j to said bulletin board apparatus to make them public, and said each user apparatus verifies said made-public hash values $h(a_j)$ and $h(b_j)$ by using said made-public random information a_j and b_j and further verifies whether $h(V_{vj}||r_i)=h(V_{vj}||a_j*b_j)$.

22. A method by which said each user apparatus in said quantitative competition method of claim 1 registers his intended value V_{vi} selected from among M integral values defined by upper and lower limits V_M and V_1 for comparison, said M being an integer equal to or larger than 2, said method comprising the steps of:

(a) responding to the input of said intended value V_{vi} to generate two M-element sequences of information s_i and t_i whose corresponding elements equal at values in the range from said value V_i or larger to said value V_{vi} or smaller and differ at values in the range from said value V_{vi} or larger to said value V_M or smaller;

(b) responding to the input of said two M-element sequences of information s_i and t_i to calculate one-way functions for said sequences of information s_i and t_i and send calculation results $H1_i$ and $H2_i$ to a bulletin board apparatus; and

(c) sending said sequence of information s_i to a first quantitative competition apparatus, said sequence of information t_i to a second quantitative competition apparatus, and said $H1_i$ and $H2_i$ to said bulletin board apparatus.

23. A method by which said each user apparatus in said quantitative competition method of claim 11 registers his intended value V_{vi} selected from among M integral values defined by upper and lower limits V_M and V_1 for comparison, said M being an integer equal to or larger than 2, said method comprising the steps of:

(a) responding to the input of said intended value V_{vi} to generate two

M-element sequences of information s_i and t_i whose corresponding elements differ at values in the range from said value V_1 or larger to said value V_{vi} or smaller and equal at values in the range from a value V_{vi+1} or larger to said value V_M or smaller;

(b) responding to the input of said two M-element sequences of information s_i and t_i to calculate one-way functions for said sequences of information s_i and t_i and send calculation results $H1_i$ and $H2_i$ to a bulletin board apparatus; and

(c) sending said sequence of information s_i to a first quantitative competition apparatus, said sequence of information t_i to a second quantitative competition apparatus, and said $H1_i$ and $H2_i$ to said bulletin board apparatus.

24. A user apparatus for use in said quantitative competition method of claim 1, comprising:

a storage part having stored therein M integral values defined by upper and lower limits V_M and V_1 for comparison;

input means for inputting an intended value V_{vi} equal to or larger than said value V_1 and equal to or smaller than said value V_M;

a sequence-of-information generating part supplied with said values V_{vi}, V_1 and V_M, for generating and outputting two M-element sequences of information s_i and t_i whose corresponding elements equal at values in the range from said lower-limit value V_1 or larger to said intended value V_{vi} or smaller and differ at values in the range from said intended value V_{vi} or larger to said upper-limit value V_M or smaller, or two M-element sequences of information s_i and t_i whose corresponding elements differ at values in the range from said lower-limit value V_1 or larger to said intended value V_{vi} or smaller and equal at values in the range from a value V_{vi+1} or larger to said upper-limit value V_M or smaller, said M being the number of values selectable as said intended value V_{vi} equal to or larger than said value V_1 and equal to or smaller than said value V_M;

a one-way function calculating part supplied with said sequences of information s_i and t_i, for calculating one-way functions for said sequences of information s_i and t_i and for outputting calculation results $H1_i$ and $H2_i$; and

a transmitting part for sending said sequence of information s_i to a first quantitative competition apparatus, said sequence of information t_i to a second quantitative competition apparatus, and said $H1_i$ and $H2_i$ to a bulletin board apparatus.

25. A user apparatus for use in said quantitative competition method of claim 11, comprising:

a storage part having stored therein M integral values defined by upper and lower limits V_M and V_1 for comparison, said M being an integer equal to or larger than 2;

input means for inputting an intended value V_{vi} equal to or larger than said value V_1 and equal to or smaller than said value V_M;

a sequence-of-information generating part supplied with said values V_{vi}, V_1 and V_M, for generating and outputting two M-element sequences of information s_i and t_i whose corresponding elements differ at values in the range from said lower-limit value V_1 or larger to said intended value V_{vi} or smaller and equal at values in the range from a value V_{vi+1} or larger to said upper-limit value V_M or smaller;

a one-way function calculating part supplied with said sequences of information s_i and t_i, for calculating one-way functions for said sequences of information s_i and t_i and for outputting calculation results $H1_i$ and $H2_i$; and

a transmitting part for sending said sequence of information s_i to a first quantitative competition apparatus, said sequence of information t_i to a second quantitative competition apparatus, and said $H1_i$ and $H2_i$ to a bulletin board apparatus.

26. A quantitative competition apparatus for use in a quantitative competition method of claim 1 or 11, comprising:

a receiving part for receiving from each user apparatus a sequence of information consisting of elements of the same number M as that of values selectable as an intended value V_{vi} in the range of between lower-limit and upper-limit values V_1 and V_M, and for receiving an integral value w from a bulletin board apparatus;

a storage part for storing said sequence of information received from said each user apparatus;

a one-way function calculating part supplied with w-th elements of said sequences of information received from users, for calculating and outputting one-way functions for concatenations of said w-th elements; and

a transmitting part for sending said calculated one-way functions to said bulletin board apparatus.

27. A competition method by a quantitative competition apparatus for use in said quantitative competition method of claim 1 or 11, said method comprising the steps of:

(a) receiving, from each user apparatus i, where =1,2,..., N, an M-element sequence of information $s_i=\{s_{i,1}\ s_{i,2}, \ldots, s_{i,M}\}$ as information representing an intended value V_{vi} selected from among M values in the range of between lower-limit and upper-limit values V_1 and V_M;

(b) receiving an integral value w from a bulletin board apparatus;

(c) inputting a w-th element $s_{i,w}$ of said sequence of information s_i received from said each user apparatus and calculating a one-way function for a concatenation of such input w-th elements $s_{i,w}$; and

(d) sending said calculated one-way function to said bulletin board.

28. A quantitative competition apparatus for use in said quantitative competition method of claim 1 or 11, said apparatus comprising:

a receiving part for receiving from each user apparatus a sequence of information consisting of elements of the same number M as that of values selectable as an intended value V_{vi} in the range of between lower-limit and upper-limit values V_1 and V_M, and for receiving an integral value w from a bulletin board apparatus;

a storage part for storing said sequence of information received from said each user apparatus;

a one-way function calculating part supplied with w-th elements of said sequences of information received from users, for calculating and outputting one-way functions for concatenations of said w-th elements; and

a transmitting part for sending said calculated one-way functions to said bulletin board apparatus.

29. A computer program for executing the procedure to be followed by a user apparatus in a quantitative competition method of claim 1 or 11, said program comprising the steps of:

responding to an intended value V_{vi} selected from among integral values defined by upper-limit and lower-limit values V_1 and V_M for comparison to generate two M-element sequences of information s_i and t_i whose corresponding elements equal at values in the range from said lower-limit value V_1 or larger to said intended value V_{vi} or smaller and differ at values in the range from said intended value V_{vi} or larger to said upper-limit value V_M or smaller, or two M-element sequences of information s_i and t_i whose corresponding elements differ at values in the range from said lower-limit value V_1 or larger to said intended value V_{vi} or smaller and equal at values in the range from a value V_{vi+1} or larger to said upper-limit value V_M or smaller, said M being the number of values selectable as said intended value V_{vi} equal to or larger than said value V_1 and equal to or smaller than said value V_M;

calculating one-way functions for said sequences of information s_i and

t_i and for outputting calculation results $H1_i$ and $H2_i$; and

sending said sequence of information s_i to a first quantitative competition apparatus, said sequence of information t_i to a second quantitative competition apparatus, and said $H1_i$ and $H2_i$ to a bulletin board apparatus.

30. A recording medium on which there is recorded said computer program of claim 29.